CLAIMS

What is claimed is:

1. A method for accepting certificates in a network, the network including a remote system and a local system, comprising the steps of:

(a) receiving a certificate issued by a third party from a remote system by a local system, wherein the certificates comprises at least one attribute;

(b) performing local due diligence at the local system on the certificate;

(c) determining if the certificate is valid based on the local due diligence; and

(d) creating an override certificate to add or modify at least one attribute of the certificate, if the certificate is determined to be valid.

2. The method of claim 1, wherein the certificate contains an identity of a remote user at the remote system.

3. The method of claim 1, wherein the performing step (b) further comprises:

(b1) determining if the third party is a trusted third party.

4. The method of claim 1, wherein the local due diligence is defined by a local user at the local system.

5. The method of claim 1, wherein the determining step (c) comprises:

(c1) determining if the certificate is valid based on the local due diligence instead of relying on a due diligence performed by the third party.

6. The method of claim 1, wherein the determining step (c) comprises:

(c1) determining if the certificate is valid based on the local due diligence and a due diligence performed by the third party.

7. The method of claim 1, wherein the at least one attribute comprises a trust level from a gradation of trust levels.

8. The method of claim 1, wherein the override certificate is an extension of the certificate issued by the third party.

9. The method of claim 1, wherein the override certificate replaces the certificate issued by the third party.

10. The method of claim 1, wherein the override certificate replaces a previously created override certificate.

11. The method of claim 1, further comprising:

(e) granting access to the local system to a remote user at the remote system according to attributes in the override certificate.

12. The method of claim 1, further comprising:

(f) denying access to the local system if the certificate is determined to be invalid.

13. A system, comprising:

a remote system connected to a network;

a local system connected to the network, wherein the local system comprises:

a certificate issued by a third party and received from the remote system, and

an override certificate, wherein the override certificate adds or modifies at least one attribute of the certificate based on local due diligence performed at the local system.

14. The system of claim 13, wherein the override certificate adds or modifies the at least one attribute of the certificate based on the local due diligence performed at the local system instead of relying on due diligence performed by the third party.

15. The system of claim 13, wherein the override certificate adds or modifies the at least one attribute of the certificate based on the local due diligence performed at the local system and a due diligence performed by the third party.

16. The system of claim 13, wherein the override certificate is an extension of the certificate issued by the third party.

17. The system of claim 13, wherein the override certificate replaces the certificate issued by the third party.

18. The system of claim 13, wherein the override certificate replaces a previously

created override certificate.

19. The system of claim 13, further comprising:

a remote user at the remote system, wherein the remote user is granted access to the local system according to attributes in the override certificate.

20. A computer readable medium with program instructions for accepting certificates in a network, the network including a remote system and a local system, comprising the instructions for:

(a) receiving a certificate issued by a third party from a remote system by a local system, wherein the certificates comprises at least one attribute;

(b) performing local due diligence at the local system on the certificate;

(c) determining if the certificate is valid based on the local due diligence; and

(d) creating an override certificate to add or modify at least one attribute of the certificate, if the certificate is determined to be valid.

21. The medium of claim 20, wherein the certificate contains an identity of a remote user at the remote system.

22. The medium of claim 20, wherein the performing instruction (b) further comprises instructions for:

(b1) determining if the third party is a trusted third party.

23. The medium of claim 20, wherein the local due diligence is defined by a local user at the local system.

24. The medium of claim 20, wherein the determining instruction (c) comprises instructions for:

(c1) determining if the certificate is valid based on the local due diligence instead of relying on a due diligence performed by the third party.

25. The medium of claim 20, wherein the determining instructions (c) comprises instructions for:

(c1) determining if the certificate is valid based on the local due diligence and a due diligence performed by the third party.

26. The medium of claim 20, wherein the at least one attribute comprises a trust level from a gradation of trust levels.

27. The medium of claim 20, wherein the override certificate is an extension of the certificate issued by the third party.

28. The medium of claim 20, wherein the override certificate replaces the certificate issued by the third party.

29. The medium of claim 20, wherein the override certificate replaces a

previously created override certificate.

30. The medium of claim 20, further comprising instructions for:

(e) granting access to the local system to a remote user at the remote system according to attributes in the override certificate.

31. The medium of claim 20, further comprising instructions for:

(f) denying access to the local system if the certificate is determined to be invalid.